UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* The property located at 1239 East Providence Loop Placentia, CA 92870	)	Case No. 8: 25-MJ-00272

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☒ evidence of a crime;

☒ contraband, fruits of crime, or other items illegally possessed;

☒ property designed for use, intended for use, or used in committing a crime;

☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A(a)(2)	Receipt and distribution of child pornography
18 U.S.C. § 2252A(a)(5)(B)	Possession of child pornography

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of_____days (*give exact ending date if more than 30 days*:_____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Payton Tidd

Applicant's signature

Payton Tidd, Special Agent HSI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: _____

Judge's signature

City and state: Santa Ana, CA

Douglas F. McCormick, United States Magistrate Judge

Printed name and title

AUSA: Melissa Rabbani 714-338-3499

AFFIDAVIT

I, Payton Tidd, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent with the United States Department of Homeland Security, Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI"), assigned to HSI Orange County, California. In 2023, I attended the Criminal Investigator Training Program, and the Homeland Security Special Agent Training Program located at the Federal Law Enforcement Training Center in Glynco, Georgia. I have participated in and/or received training in numerous investigations of criminal activity, including, but not limited to, the investigation of narcotics offenses, money laundering, fraud, child pornography, alien smuggling and human trafficking. During investigation of these matters, I have participated in the execution of search warrants.

2. I investigate, among other things, the sexual exploitation of children and child pornography in the Central District of California as part of the Orange County Child Exploitation Task Force ("OCCETF"). The OCCETF is responsible for enforcing federal criminal statutes involving the sexual exploitation of children under Title 18, United States Code, Section 2252, et seq. As part of these investigations, I have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. Moreover, I am a federal law enforcement

officer who is engaged in enforcing criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

II. PURPOSE OF AFFIDAVIT

3. This affidavit is made in support of an application for a warrant to search the premises located at 1239 East Providence Loop, Placentia, CA 92870 (the "SUBJECT PREMISES"), more fully described below and in Attachment A, and to seize evidence, fruits, and instrumentalities of criminal conduct, as specified in Attachment B, which is also attached hereto and incorporated by reference, specifically, violations of 18 U.S.C. §§ 2252A(a)(2) (receipt and distribution of child pornography) and 2252A(a)(5)(B) (possession of child pornography) (collectively, the "SUBJECT OFFENSES").

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. PREMISES TO BE SEARCHED

5. The SUBJECT PREMISES is the property located at 1239 East Providence Loop, Placentia, CA 92870(the "SUBJECT PREMISES"). The SUBJECT PREMISES is a two-story family home

with the numbers "1239" visible to the left of the attached garage. The SUBJECT PREMISES has a white exterior and brown trim with a red tile roof. The front door and garage of the SUBJECT PREMISES face east and are brown in color.

IV. DEFINITIONS

6. The following definitions apply to this affidavit and Attachment B:

a. The terms "minor," "sexually explicit conduct," "visual depiction," "producing," and "child pornography" are defined in 18 U.S.C. § 2256.

b. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. The term "computer" is defined in 18 U.S.C. § 1030(e)(1).

d. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including

keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

e. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

f. The term "Internet" is defined as the worldwide network of computers — a noncommercial, self-governing network devoted mostly to communication and research with roughly 3.2 billion users worldwide. The Internet is not an online service and has no real central hub. It is a collection of tens of thousands of computer networks, online services, and single user components. In order to access the Internet, an individual computer user must use an access provider, such as a university,

employer, or commercial Internet Service Provider ("ISP"), which operates a host computer with direct access to the Internet.

g. The term "Internet Protocol" ("IP") is defined as the primary protocol upon which the Internet is based. IP allows a packet of information to travel through multiple networks (groups of linked computers) on the way to its ultimate destination.

h. The term "IP address" is defined as a unique number assigned to each computer directly connected to the Internet (for example, 74.100.66.74). Each computer connected to the Internet is assigned a unique IP address while it is connected. The IP address for a user may be relatively static, meaning it is assigned to the same subscriber for long periods of time, or dynamic, meaning that the IP address is only assigned for the duration of that online session.

i. The term "Internet Service Provider" ("ISP") is defined as a business that allows a user to dial into or link through its computers, thereby allowing the user to connect to the Internet for a fee. ISPs generally provide only an Internet connection, an electronic mail address, and maybe Internet browsing software. A user can also connect to the Internet through a commercial online service such as AT&T, Verizon, or Time Warner Cable. With this kind of connection, the user gets Internet access and the proprietary features offered by the online service, such as chat rooms and searchable databases.

j. A "hash value" is a unique alpha-numeric identifier for a digital file. A hash value is generated by a

mathematical algorithm, based on the file's content. A hash value is a file's "digital fingerprint" or "digital DNA." Two files having identical content will have the same hash value, even if the file names are different. On the other hand, any change to the data in a file, however slight, will change the file's hash value, even if the file name is unchanged. Thus, if two files have the same hash value, they are said to be identical, even if they have different file names.

k. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

l. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

m. A "website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language ("HTML") and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol ("HTTP").

V. PROBABLE CAUSE

A. Background on NCMEC, the CyberTipline, and Kik

7. The National Center for Missing & Exploited Children ("NCMEC") is the leading non-profit organization in the U.S. working with law enforcement, families, and the professionals who serve them on issues related to missing and sexually

exploited children. NCMEC has established a missing child hotline and serves as the national clearinghouse for information related to these issues.

8. NCMEC operates a CyberTipline to provide electronic service providers an effective means of reporting Internet-related child sexual exploitation, including possession, manufacture, and distribution of child pornography. 42 U.S.C. § 5773(b)(1)(P). Any electronic service provider that discovers what appears to be child pornography must report that fact and its surrounding circumstances to the CyberTipline. 18 U.S.C. § 2258A(a). See also United States v. Keith, 980 F. Supp. 2d 33, 39 (D. Mass. 2013). NCMEC forwards information received from electronic service providers via the CyberTipline to an appropriate federal or state law enforcement agency. 18 U.S.C. § 2258A(c).

9. Kik Messenger (hereinafter "Kik") is a mobile application designed for chatting or messaging owned and operated by Kik c/o Medialab.ai Inc. According to the publicly available document, "Kik's Guide for Law Enforcement," to use this application, a user downloads the application to a mobile phone, computer, or other digital device via a service such as the iOS App Store, Google Play Store, Apple iTunes, or another similar provider. Once the application is downloaded and installed, the user is prompted to create an account and username. The user also creates a display name, which is a name that other users see when transmitting messages back and forth. Once the user has created an account, the user is able to locate

other users via a search feature. While messaging, users can then send each other text messages, images, and videos.

B. The CyberTipline Reports

10. This investigation began when, in July 2024 through August 2024, Kik submitted CyberTipline Reports 197073900, 199106519, 197914573, 199118107, 198984216, 198371299 to the NCMEC CyberTipline.

11. CyberTipline Report 197073900 reported that on July 14, 2024, at approximately 2121 hours, Kik user jerryjones7979, with the email address jerryjones77@live.com, sent a file with the file name "efa605c8-6268-4330-8a71-00933ef59633.mp4" to another user via private chat message. The file is a video that is approximately eighteen seconds in length and depicts a minor female approximately four to seven years of age. The child can be seen lying on her back wearing a striped shirt and no pants or underwear. The child's legs are spread open exposing her vagina. Throughout the video, the adult male is inserting his erect penis into the child's vagina. At the end of the video, the adult male removes his erect penis from the girl's vagina while white liquid ejects from the top of his erect penis (REPORTED VIDEO 1).

12. CyberTipline Report 198984216 reported that on July 14, 2024, at approximately 2123 hours, the same "jerryjones7979" account sent the same video, REPORTED VIDEO 1, to another user via media forwarding in a private chat message.

13. CyberTipline Report 197073900 reported that IP Address 107.139.104.235 (the "SUSPECT IP ADDRESS") was used to login to

the "jerryjones7979" Kik account on July 14, 2024, at approximately 2115 hours, roughly six and eight minutes before the "jerryjones7979" account sent REPORTED VIDEO 1 to two other users as stated above.

14. CyberTipline Report 197914573 reported that on August 5, 2024, at approximately 1704 hours, Kik user grouch8888, with the email address grouch888@live.com, sent a file with the file name "40aea9df-774d-4e6b-aedc-b8fc57404777.mp4" to another user via private chat message. This file is a video that is approximately twenty-four seconds in length and depicts a minor female approximately two to four years of age. The girl can be seen lying on her back on top of a brown surface. Throughout the video, an adult male can be seen inserting his erect penis into the anus of the minor female. At approximately seven seconds, the adult male lifts both legs of the minor female while simultaneously moving his erect penis in and out of the child's anus. For the rest of the video, the adult male can be seen holding up the legs of the child while he moves his penis in and out of the child (REPORTED VIDEO 2).

15. CyberTipline Report 199106519 reported that on August 5, 2024, at approximately 1708 hours, the same "grouch8888" account sent REPORTED VIDEO 2 to another user.

16. CyberTipline Report 197914573 reported that the SUSPECT IP ADDRESS was used to login to the "grouch8888" Kik account on August 5,2024 at approximately 1654 hours, roughly 10 and 14 minutes before the "grouch8888" account sent REPORTED VIDEO 2 to other users.

17. CyberTipline Report 198371299 reported that on August 19, 2024, at approximately 2344 hours, Kik user mikegrouch9292, with the email address mikegrouch9292@hotmail.com, sent a file with the file name "df44ddc4-b0ce-4e6f-8220-17f38d4fe7e1.mp4" to another user via private chat message. This file is a video that is approximately seven seconds in length and depicts a minor female approximately eleven to fifteen years of age. Throughout the video, the minor female is naked and is standing with one leg raised to expose her vagina. At approximately four seconds, the minor female inserts a makeup brush into her vagina. For the rest of the video, she is moving the makeup brush farther into her vagina (REPORTED VIDEO 3). CyberTipline Report 198371299 reported that the SUSPECT IP ADDRESS was used to login to the "mikegrouch9292" Kik account on August 19, 2024, at approximately 2332 hours, roughly 12 minutes before the "mikegrouch9292" account sent REPORTED VIDEO 3 to another user.

18. CyberTipline Report 199118107 reported that on August 19, 2024, at approximately 2355 hours, Kik user mikegrouch9292, with the email address mikegrouch9292@hotmail.com, sent REPORTED VIDEO 3 to another user via media forwarding in a private chat message. This file was uploaded using the SUSPECT IP ADDRESS. Additionally, CyberTipline Report 199118107 reported that the SUSPECT IP ADDRESS was used to log into the user account on August 19, 2024, at 2332 hours, roughly 23 minutes before the "mikegrouch9292" account sent REPORTED VIDEO 3 to a second user.

19. CyberTipline Reports 197073900, 197914573, and 198371299 reported that the IP address for the uploaded files

was connected to Cloudflare Warp that geolocates to Lagos, Nigeria. After further research on Cloudfare Warp, it is a Virtual Private Network (VPN) service that encrypts the user's internet activity, ultimately, hiding the identity and location of the user. Based on the timeline of when the user logged into Kik through the SUSPECT IP ADDRESS and the file uploads geolocating to Nigeria, we believe that the user was using Cloudflare Warp to hide his identity when uploading the files.

C. Identification of the SUBJECT PREMISES

20. On November 18, 2024, a Department of Homeland Security Summons was issued to AT&T Corp. to provide all subscriber records for the SUSPECT IP ADDRESS used on July 14, 2024, which was the date for the SUSPECT IP ADDRESS and ports provided by KIK on Cybertip 197073900. On November 19, 2024, AT&T responded with the following information on the subscriber for the SUSPECT IP ADDRESS: Polly Dagmy Goff, 1239 E PROVIDENCE LOOP, PLACENTIA, CA 92870-4224 (the SUBJECT PREMISES).

21. On February 24, 2025, Homeland Security Investigations (HSI) Special Agent (SA) Payton Tidd conducted law enforcement record checks for the SUBJECT PREMISES. Checks showed that Polly Dagmy-Goff and Jason Bradley Goff both resided at the SUBJECT PREMISES. SA Tidd reviewed California Department of Motor Vehicle (CA DMV) records for both Polly Dagmy-Goff and Jason Goff and learned that they both possess California driver's licenses ("CADL") which identifies their residence as the SUBJECT PREMISES. Additionally, SA Tidd acquired CADL Photos of both Polly Dagmy Goff and Jason Goff.

22. A search of public databases revealed that Jason Goff works for Mt. San Antonio College, and the website for the college, located at 1100 N Grand Ave Walnut, CA 91789, currently lists Goff as a biology professor. Additionally, the website for Stanbridge University, with an Orange County location at 2041 Business Center Dr Ste 107, Irvine, CA 92612, currently lists Jason Goff as the General Education Program Director for the Occupational Science in Occupational Therapy Assistant program.

23. Following review of CADL records, SA Tidd found two vehicles registered to Jason Goff and Polly Dagmy-Goff at the SUBJECT PREMISES. The vehicles include a blue 2023 Volkswagen Taos SE bearing California license plate "9DFH328" (SUBJECT VEHICLE 1) and a Red 2023 Chevrolet Bolt EUV LT bearing California license plate "9KRV103" (SUBJECT VEHICLE 2). Moreover, as discussed below, agents have conducted recent surveillance at the SUBJECT PREMISES and have seen the vehicles registered to Polly Dagmy-Goff and Jason Goff parked at the SUBJECT PREMISES.

24. On February 26, 2025, at approximately 0630 hours, surveillance was conducted at the SUBJECT PREMISES. At approximately 0837 hours, SA Tidd watched as a male individual matching the CADL photo of Jason Goff watered his plants in the front yard of the SUBJECT PREMISES. At approximately 0904 hours, the garage attached to the SUBJECT PREMISES opened which revealed SUBJECT VEHICLE 2 parked. At approximately 0905 hours, SA Tidd watched as a female individual matching the CADL photo of Polly Dagmy-Goff opened the door of SUBJECT VEHICLE 2. At

approximately 0908 hours, the male individual matching the CADL photo of Jason Goff walked into the garage from a side door that led to the left side of the property. At approximately 0911 hours, the female individual matching the CADL photo of Polly Dagmy-Goff got into SUBJECT VEHICLE 2, backed the vehicle out of the garage, closed the garage door and then left the premises.

25. On April 2, 2025, at approximately 0700 hours, surveillance was conducted at the SUBJECT PREMISES. At approximately 0732 hours, SA Tidd watched as a male matching the CADL photo of Jason Goff walked from the left side of the property, walked toward the street, grabbed a trashcan, and rolled the trashcan to the left side of the SUBJECT PREMISES. At approximately 0805 hours, SA Tidd watched as the garage door attached to the SUBJECT PREMISES opened revealing SUBJECT VEHICLE 2. At this time, a female matching the CADL photo of Polly Dagmy-Goff walked into the garage and began putting bags in SUBJECT VEHICLE 2, which was parked inside the garage. Shortly after, the male matching the CADL photo of Jason Goff opened a door from the left side of the SUBJECT PREMISES to the garage. The male matching the CADL photo of Jason Goff grabbed something in the garage and went back through the door to the left side of the SUBJECT PREMISES.

26. On April 4, 2025, at approximately 0934 hours, surveillance was conducted at the SUBJECT PREMISES. During this time, SA Thomas Gingell observed as SUBJECT VEHICLE 1 was parked on the street in front of the SUBJECT PREMISES.

VI. TRAINING AND EXPERIENCE RELATING TO CHILD PORNOGRAPHY AND PERSONS WHO COLLECT CHILD PORNOGRAPHY

27. Based on my training and experience, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that child pornography is readily available on the Internet, from which it can easily be downloaded onto a personal computer, smart phone, or other device with Internet access in the form of digital video and image files. Such digital files are easily saved or copied onto portable electronic data storage devices, such as external hard drives and smaller, more compact thumb and flash drives. Such digital files are also easily copied or "burned" onto CDs and DVDs and transferred onto smart phones and other types of mobile telephones and personal computing devices, such as tablets.

28. Based on my training and experience, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned the following information about the availability of child pornography on the internet and the practices of persons who distribute, possess, and collect child pornography images and videos:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, digital photographs, magazines, motion pictures, videotapes, digital videos, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse a selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals may also correspond with others with similar interests to share information and materials. In such cases, these persons rarely destroy correspondence from other child pornography distributors and possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

d. Such individuals frequently also collect and maintain materials evidencing a sexual interest in young children, such as fantasy writings and texts, emails, and chats with other people with similar interests.

e. Such individuals almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, digital videos, magazines, negatives, photographs, digital photographs, correspondence, mailing lists, books, tape recordings, etc., in

the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, digital photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, videotapes and digital videos for many years.

f. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer, an external hard drive, or a flash or thumb drive. Child pornography images stored in this way are often maintained for several years and kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Thus, even if a person suspected of possessing child pornography uses a portable device (such as a mobile phone) to access child pornography on the Internet, there is probable cause, based on my training and experience, to believe that either child pornography or evidence of accessing the Internet with intent to view child pornography will be found in his residence, as well as vehicles located at the person's residence.

g. Some possessors of child pornography have been known repeatedly to download child pornography onto their computers, view it, and then delete it from their computers. In such cases, evidence of this activity, including deleted child

pornography image and video files, often can be located on such person's computers and digital devices using forensic tools.

VII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

22. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable

data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

23. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which

may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

24. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when

a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress Polly Dagmy-Goff and Jason Goff's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of Polly Dagmy-Goff and Jason Goff's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

25. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VIII. CONCLUSION

26. For all the reasons described above, there is probable cause to believe that evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2) (receipt and distribution of child pornography), and 2252A(a)(5)(B) (possession of child pornography), as described above and in Attachment B of this affidavit, will be found in a search of the SUBJECT PREMISES, as further described above and in Attachment A of this affidavit.

/s/ Payton Tidd

Payton Tidd, Special Agent
Homeland Security
Investigations

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this ___ day of April 2025.

HONORABLE DOUGLAS F. MCCORMICK
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

PREMISES TO BE SEARCHED

The SUBJECT PREMISES is the property located at 1239 East Providence Loop, Placentia, CA 92870(the "SUBJECT PREMISES"). The SUBJECT PREMISES is a two-story family home with the numbers "1239" visible to the left of the attached garage. The SUBJECT PREMISES has a white exterior and brown trim with a red tile roof. The front door and garage of the SUBJECT PREMISES face east and are brown in color.

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2) (receipt and distribution of child pornography), and 2252A(a)(5)(B) (possession of child pornography), namely:

a. Child pornography, as defined in 18 U.S.C. § 2256(8)(A) and (C).

b. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that refer to child pornography, as defined in 18 U.S.C. § 2256(8)(A) and (C), including documents that refer to the possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, or downloading, production, shipment, ordering, requesting, or trading of child pornography, or documents that refer to a transaction of any kind involving child pornography.

c. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, tending to identify persons involved in the possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, or downloading, production, shipment, ordering, requesting, or trading of child pornography, or involved in a

transaction of any kind involving child pornography, as defined in 18 U.S.C. § 2256(8)(A) and (C).

d. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that identify any minor visually depicted while engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

e. Any and all records, documents, programs, applications, materials, or items that are sexually arousing to individuals who are interested in minors, but that are not in and of themselves obscene or that do not necessarily depict minors involved in sexually explicit conduct. Such material is commonly known as "child erotica" and includes written materials dealing with child development, sex education, child pornography, sexual abuse of children, incest, child prostitution, missing children, investigative techniques relating to child exploitation, sexual disorders, pedophilia, nudist publications, diaries, and fantasy writings.

f. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that pertain to accounts with any Internet Service Provider.

g. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, regarding ownership and/or possession of 1239 E Providence Loop, Placentia, CA 92870 (the SUBJECT PREMISES).

h. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the SUBJECT OFFENSES, and forensic copies thereof.

i. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as

telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed one year from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic

image(s) thereof beyond this one year period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques, including to search for known images of child pornography.

c. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items

to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been

able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. This warrant authorizes a review of electronic storage media seized, electronically stored information, communications, other records and information seized, copied or disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

6. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

7. During the execution of this search warrant, law enforcement is permitted to: (1) depress Polly Dagmy Goff and Jason Goff's thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct

which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of Polly Dagmy-Goff and Jason Goff's face with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

8. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.